

Application Serial No. 09/685,285

REMARKS

The Applicants and the undersigned thank Examiner Ha for her time and consideration given during the telephone interview of May 18, 2005. The Applicants also appreciate Examiner Ha's careful review of this application. Claims 1-65 have been rejected. Upon entry of this amendment, Claim 10 has been cancelled and Claims 1-9, and 11-65 remain pending in this application.

The independent claims are Claims 1, 42, 51, and 56. Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks.

Summary of Telephonic Interview of May 18, 2005

The Applicants and the undersigned thank the Examiner for her time and consideration given during the telephonic interview of May 18, 2005. During this telephonic interview, a proposed amendment to the claims was discussed. The Applicants provided the proposed amendment to the claims in advance of the interview.

The Applicants' representative explained that the prior art of record, especially U.S. Patent No. 6,070,190 issued to Reps et al. (hereinafter the "Reps" reference) and the printed publication entitled, "Signed and delivered: An Introduction to Security and Authentication; Find Out How The Java Security API can Help You Secure Your Code," authored by Todd Sundsted and published on December 1, 1998 (hereinafter the "Sundsted" reference) did not provide any teaching of classifying computer security incident information and then suggesting a procedure or tool based on a classification of the computer security information, as recited in amended independent Claims 1, 42, and 56. Regarding amended independent Claim 51, the Applicants' representative explained that this claim was amended to further emphasize that the computer locations of this claim are associated with identifying devices that are able to perform computer security steps

The focus of the interview was to make sure that Examiner Ha was comfortable with the new language of the claims and that she understood what the Applicants were trying to claim. Examiner Ha acknowledged the changes and that she understood the new language. Examiner Ha indicated that an update search would likely be needed if the

Application Serial No. 09/685,285

Applicants formally submitted an After-Final amendment. The Applicants' representative indicated that an RCE would likely be filed so that the After-Final amendment would be formally entered into the application.

The Applicants and the undersigned request Examiner Ha to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date next to this summary in the margin as discussed in MPEP § 713.04, p. 700-202.

Claim Rejections under 35 U.S.C. §112, first paragraph

The Examiner rejected Claims 1-2 and 4-65 under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement. Specifically, the Examiner found that Claims 1, 42, 51, and 56 as amended by the response of August 8, 2004 includes new subject matter.

The Examiner stated that the specification failed to discuss the claimed phrase, "the computer security incident information indicating one of suspicious computer activity that occurs *prior* to a computer security threat and an actual computer security threat." The Examiner rejected the remaining claims because of their dependencies. The Applicants respectfully offer remarks to traverse these pending rejections.

The Applicants respectfully submit that the claimed phrase identified by the Examiner above (with the emphasis by the Examiner on the word, "prior") is clearly supported by several passages of the originally filed application. Specifically, there are at least two passages that support the claimed phrase listed above:

First, the following passage mentions an incident status attribute that can be used to classify suspicious computer activity before the activity becomes a computer security threat:

"The incident status attribute can include the following values: In Progress, Not In Progress, Unknown. The incident status can measure whether the attack is in progress or not." See page 23, lines 7-8 of the originally filed application.

Second, the following passage explains that the security management system 20 can profile sequences of suspicious computer activity prior to a computer security threat to predict future actions of a source of suspicious computer activity:

Application Serial No. 09/685,285

“Once the security management system 20 accumulates sequence of actions taken by a source of a computer security incident, the security management system 20 can profile the source of the computer security incident. The profiling subsystem of the security management system 20 could match the accumulated sequences to prototypical sequences. This profiling could be used to predict future actions that a source of a computer security incident could take or help to identify the source behind a computer security incident...” See originally filed application, page 50, lines 5-10.

In light of the above passages, one of ordinary skill in the art recognizes that the claimed phrase of, “the computer security incident information indicating one of suspicious computer activity that occurs *prior* to a computer security threat and an actual computer security threat,” is clearly supported at least the two passages identified above that are part of the originally filed patent application. And therefore, this phrase does not constitute new matter. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Claim Rejections under 35 U.S.C. §§ 102(e) and 103(a)

The Examiner rejected Claims 1-2 and 4-65 under 35 U.S.C. § 102(e) as being anticipated by the Reps reference. The Examiner rejected Claims 3 under 35 U.S.C. § 103(a) as being obvious in view of the Reps reference in view of a printed publication entitled, “Signed and delivered: An Introduction to Security and Authentication; Find Out How The Java Security API can Help You Secure Your Code,” authored by Todd Sundsted and published on December 1, 1998 (hereinafter the “Sundsted” reference). The Applicants respectfully offer remarks to traverse these pending rejections.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Reps and Sundsted references fail to describe, teach, or suggest the combination of (1) recording computer security incident information with at least one of a date and time stamp, the computer security incident information indicating one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security

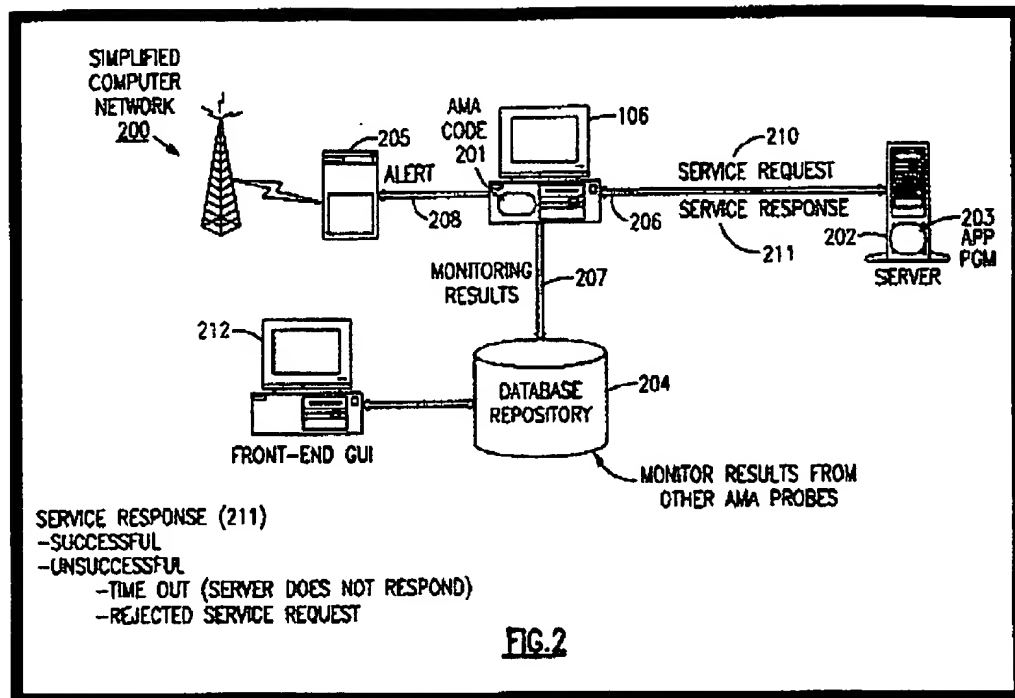
Application Serial No. 09/685,285

threat; (2) classifying the computer security incident information; (3) suggesting a procedure based on a classification of the computer security incident information; (4) providing data to enable display of a procedure comprising one or more steps for one of investigating and responding to the computer security incident information; (5) receiving a selection of one or more steps of a procedure; (6) executing the selected one or more steps of the procedure; (7) in response to executing the one or more steps of the selected procedure, recording executed procedure information and results of the executed one or more steps of the procedure with at least one of a date and time stamp; and (8) outputting a record comprising the computer security incident information, executed procedure information, results of one or more steps of the executed procedure, an identity of a user who selected the procedure, and at least one of a corresponding date stamp and time stamp, as recited in amended Claim 1.

The Reps reference describes technology that is in the field of network system service, and particularly to an end-user based application availability and response monitoring and alerting system. The technology described by the Reps reference enables the monitoring of availability of response time or other desired performance metrics of an application program from the perspective of an end-user utilizing an application program over a distributed computing network. See the Reps reference, column 1, lines 24-31.

The Reps reference explains that a server computer 202 having an application program 203 provides application services to a client computer system 106 in which the client computer system 106 records information related to the performance of the services of the application program 203 via an application probe software 201 residing on the client computer system 1-6. See Figure 2 reproduced below and in column 5, lines 17-22 of the Reps reference.

Application Serial No. 09/685,285



Specifically, as illustrated in Figure 2 above, an application monitoring alerting (AMA) probe 201 can establish a session with a server computer 202 by requesting the services of an application program 203 operating on the server computer 202. The server computer's application program 203 provides a service response 211 over a network link 206 back to the requesting AMA probe 201. See the Repts reference, column 9, lines 58-68.

The system described by the Repts reference may include both a local and remote data repository 204 which collects probe data from a number of probes monitoring different applications at different points on a distributed computing network 100. The centralized database repository 204 records transaction records from multiple probes 201 on the network 200 and may be designed to accessible to any user of the distributed computing network 200. See the Repts reference, column 10, lines 62 through column 11, line 5.

The Repts reference does not provide any teaching of recording computer security incident information with at least one of a date and time stamp in which the computer security incident information indicates one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat. ***Further,

Application Serial No. 09/685,285

the Reps reference fails to classify the computer security incident information; suggesting a procedure based on a classification of the computer security incident information; and enable a display of the procedure comprising one or more steps for one of investigating and responding to the computer security incident information.

Instead of computer security incident information, the Reps reference is primarily concerned with the level of service and performance of an application program 203 residing on a server 202. The Examiner directs the Applicants attention to Column 14, lines 55-57 of the Reps reference as a teaching of computer security incident information indicating one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat. However, these passages only discuss performance criteria associated with a level of service:

“This would be the case, for example, wherein alerting of violation of performance criteria is desired from the probe or wherein only real time transaction information is of interest to the network administrator.” See Reps reference, column 14, lines 55-57.

One of ordinary skill in the art recognizes that the passages above do not address computer security incident information indicating one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat.

The Reps reference provides a tool to diagnose and fix programs that are not running properly or in an optimal manner. The reference is not at all concerned with any type of computer security threat or suspicious activity that occurs prior to a computer security threat.

The Examiner alleges that column 10, lines 28-56, and column 14, lines 10-15 of the Reps reference teach security incident information. As noted above, amended Claim 1 recites computer security incident information. Notwithstanding this difference, the Applicants submit that this portion of the Reps reference does not provide any teaching of either security incident information or computer security incident information. In other words, the “service response” of the Reps reference does not relate to computer security incident information, and especially computer security incident information indicating one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat.

Application Serial No. 09/685,285

Column 10, lines 28-56 of the Reps reference states the following:

“Turning to a more detailed consideration of FIG. 2, it is noted that the AMA probe 201 may receive a number of different types of service responses from the server computer 202. For example, if the application program 203 on the server computer 202 properly responds to the service request, the AMA probe 201 will receive an indication of a successfully completed request i.e., a successful service response, from the server computer 202. Alternatively, if the server computer 202 is unavailable to respond to the service request 210, the request will timeout after a predetermined period and the AMA probe 201, based upon receiving back no response for the time out period, will record that the server computer was not available. This can be viewed as an unsuccessful service response 211. Finally, if the server computer 202 rejects the service request 210 the AMA probe will again record the transaction as an unsuccessful service response 211. A rejected service request 210 may correspond to a variety of different situations, such as, wherein the client is not authorized to access the particular server or application program 203 thereon, or wherein the application program 203 has been temporarily taken ‘off-line’ for maintenance purposes or if the application program 203 is functioning improperly for any number of reasons.

Whether it is successful or unsuccessful, the service response 211 from the application program 203 on the server computer 202 (including the determination of a no-response time-out) is received at the AMA probe 201, which then records the results of the transaction in a database repository 204.”

Column 14, lines 10-15 of the Reps reference states the following:

“In determining the cycle duration, a timer mechanism 307 is included in the AMA probe code 303. In a preferred embodiment of the invention the timer mechanism 307 may simply be a mechanism which places a time signature on the initial service request 210 from the probe 201 and another time signature on the service response 211 at the probe 201 and which records the difference between these two time signatures in a transaction record 311.”

One of ordinary skill in the art recognizes that the aforementioned excerpts of the Reps reference do not relate in anyway to computer security information or even security

Application Serial No. 09/685,285

information. Instead, these passages merely describe the monitoring of "service requests" of a computer system for the purposes of logging its performance at a particular point in time.

The passages listed above relied upon by the Examiner make it evident that the Reps reference does not provide data to enable display of a procedure comprising one or more steps for one of investigating and responding to the computer security incident information, as recited in amended Claim 1. Opposite to Claim 1, the Reps reference merely records the response 211 from the application program 203, whether the service request 210 was successful or unsuccessful. The Reps reference is not concerned with why a service request 210 may not have been successful. The Reps reference does not provide a procedure for investigating or responding to computer security incident information.

And it follows that the Reps reference does not output a record comprising the computer security incident information, executed procedure information, results of one or more steps of the executed procedure, an identity of a user who selected the procedure, and at least one of a corresponding date stamp and time stamp, as recited in amended Claim 1.

The Applicants remind the Examiner that for a rejection based upon 35 U.S.C. § 102, MPEP § 2131 (8th Ed., Rev. 2, May 2004) states:

TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM...The identical invention must be shown in as complete detail as is contained in the claim. Richardson v. Suzuki Motor Co., 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989)."

The Applicants submit that the Examiner has not shown the identical invention in as complete detail as is contained in amended independent Claim 1. Because the Reps reference does not teach any aspects of computer security, the Applicants submit that this reference fails to teach numerous elements recited in independent Claim 1 and therefore, the Reps reference fails to anticipate amended independent Claim 1.

The Examiner admits that the Reps reference fails to provide a teaching of a digital signature in connection with results that are recorded by computer system as

Application Serial No. 09/685,285

recited in dependent Claim 3. To make up for this digital signature deficiency, the Examiner relies upon the Sundsted reference.

The Sundsted reference describes a digital signature that can be generated from a message in connection with sending an e-mail message. The Sundsted reference explains that a good digital signature algorithm guarantees that a digital signature can't be forged assuming the private key is secret, and that the signature is good for only the message from which it is generated. See the Sundsted reference, abstract, third paragraph.

While the Sundsted does provide an isolated teaching on digital signatures as understood by one of ordinary skill in the art, similar to the Reps reference, the Sundsted reference does not provide any computer security context. In other words, like the Reps reference, the Sundsted reference is not at all concerned with any type of computer security threat or suspicious activity that occurs prior to a computer security threat. The Sundsted reference does not provide any teaching for either investigating or responding to computer security incident information.

In light of the differences between Claim 1 and the Reps and Sundsted references, one of ordinary skill in the art recognizes that these prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of the rejection of Claim 1 are respectfully requested.

Independent Claim 42

The rejection of Claim 42 is respectfully traversed. It is respectfully submitted that the Reps and Sundsted references, fail to describe, teach, or suggest the combination of (1) providing data to enable display of one or more computer security investigation procedures for investigating one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat; (2) providing data to enable display of one or more computer security response procedures for responding to one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat; (3) in response to a selection of a computer security investigation procedure, providing data to enable display of one or more corresponding investigation steps; (4) in response to a selection of a computer security response

Application Serial No. 09/685,285

procedure, providing data to enable display of one or more corresponding response steps; and (5) generating a permanent record comprising computer security incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps, as recited in amended Claim 42.

As noted above with respect to independent Claim 1, neither the Reps reference nor the Sunsted reference relate in any way to suspicious computer activity that occurs prior to a computer security threat or an actual computer security threat; as recited in amended Claim 42. The Reps reference is merely concerned with logging performance of a computer and ways to diagnose or improve performance. The Sunsted reference provides only a general teaching of digital signatures using private and public keys. Neither reference provides display of one or more computer security investigation and response procedures for suspicious computer activity or actual computer security threats.

In light of the differences between Claim 42 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 42. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 51

The rejection of Claim 51 is respectfully traversed. It is respectfully submitted that the Reps and Sunsted references, fail to describe, teach, or suggest the combination of (1) accessing a table comprising computer locations, Internet address ranges, and computer security step information for one of investigating and responding to one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat; (2) comparing a computer security step to be executed and a target Internet address with computer locations and Internet address ranges listed in the table; (3) determining if a match exists between an Internet address of a computer security incident and the Internet address ranges listed in the table; and (4) selecting a computer to execute the computer security step based upon the matching steps, wherein

Application Serial No. 09/685,285

the computer has a location and is capable of interacting with the Internet address of the computer security incident, as recited in amended Claim 51.

As noted above with respect to independent Claim 1, neither the Reps reference nor the Sunsted reference relate in any way to suspicious computer activity that occurs prior to a computer security threat or an actual computer security threat; as recited in amended Claim 51. The Reps reference is merely concerned with logging performance of a computer and ways to diagnose or improve performance. The Sunsted reference provides only a general teaching of digital signatures using private and public keys. Neither reference provides steps for investigating or responding to either suspicious computer activity that occurs prior to a computer security threat or an actual computer security threat.

In light of the differences between Claim 51 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 51. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Application Serial No. 09/685,285

Independent Claim 56

The rejection of Claim 56 is respectfully traversed. It is respectfully submitted that the Reps and Sunsted references, fail to describe, teach, or suggest the combination of (1) receiving computer security incident information indicating one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat; (2) displaying one or more tools for one of investigating and responding to computer security incident information; (3) receiving a selection of a tool; (4) in response to a selection of a tool, forwarding data for execution of the tool; and (5) forwarding data for generating a permanent record comprising computer security incident information, executed tool information, and corresponding date and time stamps, as recited in amended Claim 56.

As noted above with respect to independent Claim 1, neither the Reps reference nor the Sunsted reference relate in any way to suspicious computer activity that occurs prior to a computer security threat or an actual computer security threat; as recited in amended Claim 56. The Reps reference is merely concerned with performance of a computer and ways to diagnose or improve performance. The Sunsted reference provides only a general teaching of digital signatures using private and public keys. Neither reference displays one or more tools for one of investigating and responding to computer security incident information.

In light of the differences between Claim 56 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 56. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 2-41, 43-50, 52-55, and 57-65

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references.

The Applicants also respectfully submit that the recitations of dependent Claims 2-41, 43-50, 52-55, and 57-65 are of patentable significance.

Application Serial No. 09/685,285

Specifically, with respect to dependent Claim 35, the Applicants respectfully submit that neither the Reps reference nor the Sundsted reference provide any teaching of predefined attributes of computer security incident information that comprise any one of a (1) computer incident severity level, (2) a computer incident category, (3) a computer incident scope value, (4) a computer incident status value, (5) an attacker internet protocol (IP) address value, (6) an attacker ISP name, (7) an attacker country, (8) an external attacker status value, (9) an incident type value, (10) a vulnerabilities level, (11) an entry point value, (12) an attack profile value, (13) a target networks value, (14) a target firewalls value, (15) a target hosts value, (16) a target services value, (17) a target accounts value, and (18) a damage type value

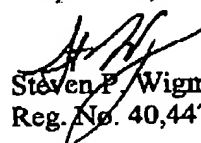
Accordingly, reconsideration and withdrawal of the rejections of the dependent Claim 35 and the other remaining dependent claims are respectfully requested.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on May 6, 2004. The Applicants and the undersigned thank Examiner Ha for the consideration of these remarks. The Applicants have submitted remarks to traverse the rejections of Claims 1-65. The Applicants respectfully submit that the present application is in condition for allowance. Such Action is hereby courteously solicited.

If any issues remain that may be resolved by telephone, the Examiner is requested to call the undersigned at 404.572.2884.

Respectfully submitted,


Steven P. Wigmore
Reg. No. 40,447

King & Spalding LLP
45th Floor
191 Peachtree Street, N.E.
Atlanta, Georgia 30303
404.572.4600
K&S Docket: 05456-105008